



19 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

12 **Offenlegungsschrift**
10 **DE 100 39 434 A 1**

51 Int. Cl. 7:
H 04 M 15/28
H 04 M 17/00
H 04 Q 7/32
// H04L 12/14

21 Aktenzeichen: 100 39 434.5
22 Anmeldetag: 11. 8. 2000
43 Offenlegungstag: 21. 2. 2002

DE 100 39 434 A 1

71 Anmelder:
Infineon Technologies AG, 81669 München, DE
73 Vertreter:
Epping, Hermann & Fischer, 80339 München

72 Erfinder:
Söhn, Anja, 81549 München, DE; Wedel, Armin,
86415 Mering, DE

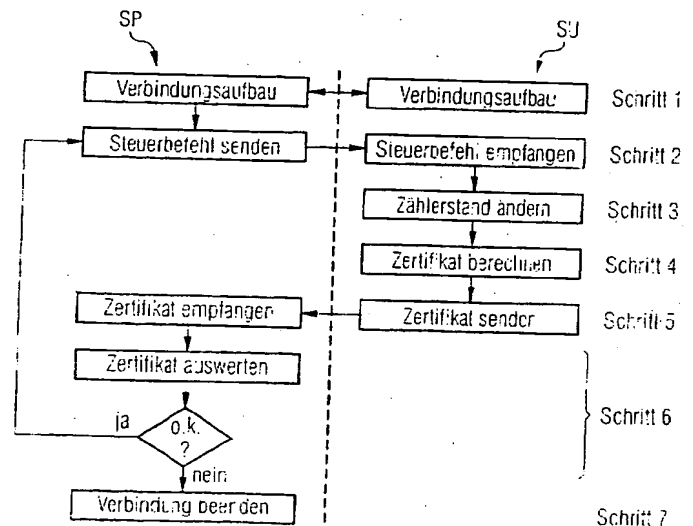
56 Entgegenhaltungen:
US 52 64 689
WO 98 59 324 A2
WO 98 18 251 A2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

54 Netzwerkanordnung und Verfahren zur Abrechnung von Dienstleistungen in einem Netzwerk

57 Die Erfindung betrifft eine Netzwerkanordnung mit einem Kommunikationsnetzwerk (1), das eine Kontrolleinrichtung (8) aufweist oder damit verbunden ist, und einem Kommunikationsendgerät (3). Außerdem betrifft die Erfindung ein Verfahren zur Abrechnung von Dienstleistungen in einem Netzwerk. In dem Netzwerk soll nach dem Prepaid-Verfahren abgerechnet werden. Dabei wird ein Datenträger (9) in dem Endgerät des Dienstanwenders (SU) verwendet, der einen Zähler (10) aufweist. Eine Kontrolleinrichtung (8) des Diensteanbieters (SP) sendet Steuerbefehle an den Datenträger (9), der daraufhin den Zählerstand ändert. In einer vorteilhaften Ausgestaltung sendet der Datenträger (9) ein Antwortsignal an die Kontrolleinrichtung (8).



DE 100 39 434 A 1

Beschreibung

[0001] Die Erfindung betrifft eine Netzwerkanordnung mit einem Kommunikationsnetzwerk, das eine Kontrolleinrichtung aufweist oder damit verbunden ist, und einem Kommunikationsendgerät. Außerdem betrifft die Erfindung ein Verfahren zur Abrechnung von Dienstleistungen in einem Netzwerk. In dem Netzwerk soll nach dem Prepaid-Verfahren abgerechnet werden.

[0002] Bisher ist es beispielsweise aus der WO 00/05684 A2 bekannt, in dem Netzwerk ein zentrales Guthabenkonto zu führen, von dem entsprechend beispielsweise einer Verbindungsdauer Guthabenbeträge abgebucht werden. Zwischen dem Dienstanbieter und dem Dienstnutzer besteht ein vertragliches Verhältnis. Bei dem Dienstanbieter wird eine sogenannte Heimatdatenbank, das Home Location Register (HLR), geführt. Das nutzungsabhängige Entgelt wird in Echtzeit von dem Guthabenkonto abgebucht, so daß eine Verbindung abgebrochen werden kann, sobald das Guthaben verbraucht ist. Hierzu ist es allerdings notwendig, eine ständige logische Verbindung zwischen dem Dienstanbieter und dem Home Location Register, beziehungsweise dem Guthabenkonto, aufrechtzuerhalten, solange der Dienstnutzer einen Dienst in Anspruch nimmt. Dies ist sehr aufwendig, so daß solche Prepaid-Dienste zur Zeit nicht für beispielsweise International-Roaming angeboten werden. Mit steigender Anzahl der Dienstanbieter entsteht außerdem ein Beziehungsgeflecht zwischen Dienstanbietern, zentralen Guthabenkonten und mobilen Dienstnutzern, das nur sehr aufwendig handhabbar ist.

[0003] Andere Prepaid-Lösungen mit netzzentrierten Konten verzichten auf eine Echtzeitabrechnung, um die Netzlast zu verringern. Hierbei werden am Ende einer Dienstnutzung sog. "Call Detail Records" (CDRs) erstellt, aus denen die Gebührendaten hervorgehen, die man dann zum entsprechenden Entwerten des Prepaid-Kontos verwendet. Hierbei kann der Netzbetreiber allerdings einen Schaden erleiden, wenn das Prepaid-Guthaben kleiner ist als die abschließenden CDR-Gebühren.

[0004] Aufgabe der Erfindung ist es daher, eine Netzwerkanordnung anzugeben, bei der die Abrechnung einfacher ist. Außerdem soll ein Verfahren zur Abrechnung von Dienstleistungen zwischen einem Dienstanbieter und einem Dienstnutzer angegeben werden, das besonders einfach und kostengünstig ist. Außerdem ist es Aufgabe der Erfindung, die Netzwerkanordnung beziehungsweise das Verfahren so zu gestalten, daß die Identität des Dienstnutzers gegenüber dem Dienstanbieter unbekannt bleibt.

[0005] Diese Aufgabe wird erfindungsgemäß bezüglich einer Netzwerkanordnung der eingangs genannten Art dadurch gelöst, daß das Mobilfunkendgerät einen Datenträger mit einem Zähler aufweist, wobei der Stand des Zählers durch einen Steuerbefehl von der Kontrolleinrichtung änderbar ist.

[0006] Die vorgeschlagene Lösung unterscheidet sich von dem heute bereits angewandten "handset-based prepaid approach"-Verfahren, bei dem auf der SIM-Karte (Subscriber Identification Module) ein Guthaben gespeichert ist, das entsprechend einer GSM Phase 2 - Zusatznachricht "Advice of Charge" (AoC) reduziert wird, was meist auf Basis einer Kostenschätzung geschieht. Die vorgeschlagene Lösung sieht vielmehr vor, daß gemäß eines vorher vereinbarten Taktes der Zähler auf einer von einem Service Provider ausgegebenen Chipkarte kontinuierlich reduziert wird und jeweils ein Zählerzertifikat in Form eines Datenpakets zur Kontrolleinrichtung transferiert wird. Die Karte ist dediziert auf den Dienst des Service Providers und enthält einen eigenen Schlüssel des Service-Providers (SP-Schlüssel). Dieser

SP-Schlüssel wird bei der Kartenpersonalisierung auf den Datenträger geschrieben und muß nicht über das Netzwerk transportiert werden.

[0007] Dadurch, daß sich der Zähler in dem Kommunikationsendgerät befindet, ist keine permanente logische Verbindung zwischen dem Kommunikationsendgerät und der Kontrolleinrichtung notwendig. Der Kostenzähler läuft immer dort, wo der Dienst in Anspruch genommen wird, also beim Benutzer. Dabei ist es unerheblich, ob sich der Nutzer beispielsweise in seinem nationalen Mobilfunknetz befindet oder über ein Mobilfunknetz eines anderen Landes mit dem heimischen Mobilfunknetz verbunden ist. Die Kontrolleinrichtung kann dem Kommunikationsnetzwerk direkt zugeordnet und zur Abrechnung der Kommunikationsverbindung selber ausgelegt sein. Sie kann aber auch zur Verrechnung von Mehrwertdiensten des Kommunikationsnetzwerkbetreibers oder von mit dem Kommunikationsnetzwerk verbundenen Dienstanbietern eingerichtet werden.

[0008] Daten zur Steuerung des Zählers können zwischen der Kontrolleinrichtung und dem Datenträger paketweise ausgetauscht werden. Da sich das Guthabenkonto, nämlich der Zähler, beim Mobilfunkendgerät befindet, muß dem Dienstanbieter die Identität des Nutzers nicht bekannt sein, sondern bleibt vergleichbar mit einer konventionellen Telefonkarte für das Festnetz anonym.

[0009] In einem erfindungsgemäßen Verfahren zur Abrechnung von Dienstleistungen zwischen einem Dienstanbieter und einem Dienstnutzer in einem Netzwerk wird ein Datenträger durch den Dienstnutzer verwendet, wobei der Datenträger einen Zähler aufweist und der Dienstanbieter einen Steuerbefehl an den Datenträger sendet, um dadurch den Stand des Zählers nach festgelegten Kriterien zu ändern.

[0010] In einer vorteilhaften Ausgestaltung der Erfindung sendet der Datenträger nach der Änderung des Zählerstandes ein Antwortsignal an den Dienstanbieter. Dadurch kann seitens des Dienstanbieters sichergestellt werden, daß der gesendete Befehl ausgeführt worden ist. Besonders vorteilhaft ist es, wenn das Antwortsignal von einem auf dem Datenträger gespeicherten Schlüssel abhängt.

[0011] Eine weitere Verbesserung der Sicherheit ergibt sich, wenn jeder Steuerbefehl eine Kennzahl aufweist, die mit dem Antwortsignal zurückgesendet wird, wobei anhand des Zeitunterschiedes zwischen Absenden und Empfangens der Signale die Verarbeitungszeit des Datenträgers ermittelt werden kann. Softwareemulationen von Datenträgern sind somit erkennbar.

[0012] In einer günstigen Ausführung der Erfindung kann der Zählerstand durch die Zahlung eines Geldbetrages an den Dienstanbieter auf einen neuen Anfangszählerstand gesetzt werden, während in einer einfachen Ausgestaltung der Datenträger beim Kauf einen bestimmten Zählerstand aufweist und nach dessen Verbrauch unbrauchbar ist.

[0013] Von besonderem Vorteil für die Sicherheit ist es, wenn neben dem Geldzähler auf der Karte noch ein redundanter Zähler in einer Netzwerkdatenbank mitgeführt wird. Dieser redundante Zähler muß nicht in Echtzeit aktualisiert werden, sondern wird jeweils nach Beendigung der Dienstanspruchnahme an den Kartenzähler angepaßt. Sobald ein Quercheck des Kartenzählers mit dem Redundanzzähler im Netzwerk zeigt, daß der Kartenzähler einen höheren Wert als der Redundanzzähler ausweist, liegt der Verdacht einer Kartenmanipulation vor und es lassen sich entsprechende Maßnahmen einleiten. Zur leichteren Auffindbarkeit des Netzwerkdatenbank-Zählers ist es weiterhin von Vorteil, wenn ein Adreßzeiger auf dem Datenträger gespeichert ist. Damit kann der Quercheck zwischen dem Kartenzähler und dem Netzwerkzähler beschleunigt werden. Mit dem redundanten Netzwerkdatenbank-Zähler kann auch vorteilhaft

eine weitere Sicherheitsmaßnahme gegen Mißbrauch realisiert werden. Es wird dazu vorgeschlagen, neben dem Geldzähler auch Information über den Zeitpunkt der Dienstanspruchnahme und über den Ort der Dienstanspruchnahme (z. B. Location Area Identity, LAI) abzuspeichern. Diese Location Area Identity kann auch in eine Zertifikatsberechnung einbezogen werden. Auf diese Weise kann der Nachweis erbracht werden, daß eine mißbräuchlich duplizierte Karte gleichzeitig an zwei Stellen im Netzwerk benutzt wurde.

[0014] Zusätzlich kann vorgesehen werden, daß die Karte einen Mechanismus enthält, mit der eine Karte nach Verbrauch beziehungsweise generell nach Ablauf ihrer Gültigkeit unbrauchbar gemacht wird.

[0015] Weitere Einzelheiten und Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

[0016] Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels näher erläutert. Es zeigt:

[0017] Fig. 1 eine Netzwerkordnung nach der Erfindung.

[0018] Fig. 2 ein Ablaufdiagramm eines erfindungsgemäßen Verfahrens zur Abrechnung in einer ersten Ausführung.

[0019] Fig. 3 ein Ablaufdiagramm eines erfindungsgemäßen Verfahrens zur Abrechnung in einer zweiten Ausführung und

[0020] Fig. 4 und Fig. 5 erfindungsgemäße Teilverfahren zur Kontrolle der Verarbeitungszeit bei der Zertifikatsberechnung.

[0021] In einem Ausführungsbeispiel, das in der Fig. 1 dargestellt ist, wird ein Mobilfunknetz 1 durch einen Netzbetreiber zur Verfügung gestellt und ist zur Kommunikation von Mobilfunkendgeräten 3 untereinander sowie mit anderen Kommunikationspartnern vorgesehen. Die Verbindungen werden über Vermittlungsstellen 2 abgewickelt. Die Verbindung zwischen der Vermittlungsstelle 2 und dem Mobilfunkendgerät 3 ist zum Teil leitungsgelassen, nämlich bis zu einer Sendestation 4, und erfolgt zum anderen Teil über eine Funkverbindung 5 zwischen der Sendestation 4 und dem Mobilfunkendgerät 3. Die Abrechnung zwischen einem Dienstnutzer, der in Besitz des Mobilfunkendgerätes 3 ist und dem Betreiber des Mobilfunknetzes 1 erfolgt im herkömmlichen Verfahren und ist vertraglich geregelt. Zur Authentisierung des Dienstnutzers ist in dem Mobilfunkendgerät 3 eine SIM-Karte 6 (Subscriber Identity Modul) enthalten. Weiterhin ist mit dem Mobilfunknetz 1 ein Dienstanbieter 7 gekoppelt, der über das Mobilfunknetz 1 erreichbar ist. Der Dienstanbieter 7 bietet über den Betreiber des Mobilfunknetzes 1 Zusatzdienste, sogenannte Mehrwertdienste, an. Der Dienstanbieter verfügt über eine Kontrolleinrichtung 8, die für die Abrechnung der erbrachten Dienstleistung zuständig ist. Als Gegenpart zu der Kontrolleinrichtung 8 ist in dem Mobilfunkendgerät 3 ein Datenträger 9 vorgesehen, der einen Zähler 10 aufweist. Über das Mobilfunknetz 1 kann die Kontrolleinrichtung 8 einen Steuerbefehl an den Datenträger 9 senden, der daraufhin den Stand des Zählers 10 ändert.

[0022] In der Fig. 2 ist detailliert dargestellt, wie das Verfahren zur Abrechnung zwischen dem Dienstnutzer (SU) und dem Dienstanbieter (SP) abläuft. Zunächst wird über das Mobilfunknetz 1 eine Verbindung zwischen dem Dienstnutzer SU und dem Dienstanbieter SP aufgebaut (Schritt 1). Sobald der Dienstnutzer (SU) die Dienstleistung in Anspruch nimmt, übermittelt der Dienstanbieter SP einen Steuerbefehl an den Dienstnutzer SU (Schritt 2). Der Datenträger, beispielsweise eine Chipkarte, der den Steuerbefehl empfängt, ändert daraufhin den Zählerstand des eingebauten Zählers entsprechend dem Steuerbefehl (Schritt 3). Nach der Änderung des Zählerstandes berechnet der Datenträger ein

Zertifikat (Schritt 4). Das Zertifikat soll dem Dienstanbieter bestätigen, daß der Zählerstand geändert wurde. Um Fälschungen des Datenträgers zu vermeiden, erfolgt die Zertifikatsberechnung unter Verwendung eines auf dem Datenträger gespeicherten Schlüssels. Das Zertifikat wird anschließend an den Dienstanbieter SP übermittelt (Schritt 5). Im Schritt 6 wird das Zertifikat ausgewertet, beispielsweise überprüft, ob das Zertifikat zu dem von dem Zähler abzuhenden Betrag paßt. Weiterhin wird überprüft ob der Schlüssel gültig ist. Für die Auswertung des Zertifikats ist eine Vielzahl von Möglichkeiten gegeben, wobei je nach gewünschter Sicherheitsstufe die Sicherheitsmaßnahmen gewählt werden. Wenn das Zertifikat nicht in Ordnung ist oder den Dienstanbieter nicht erreicht, wird die Verbindung zu dem Dienstnutzer unterbrochen (Schritt 7). Andernfalls wird nach einer bestimmten verstrichenen Zeit oder der Erfüllung anderer Kriterien ein weiterer Steuerbefehl an den Dienstnutzer übermittelt.

[0023] Die Anonymität des Benutzers bleibt in jedem Fall gewahrt, wenn ein solcher Datenträger als Prepaid-Karte anonym gegen Barzahlung verkauft wird. Der Dienstnutzer muß keinen Zugriff auf sein Endgerät gestatten. Anhand eines Aufdrucks auf der Karte ist in vorteilhafter Ausführung des Datenträgers erkennbar, für welche Dienste die Karte gültig ist. Mehrere Dienstanbieter können zur Herausgabe einer gemeinsamen Karte zusammenarbeiten. Der Dienstanbieter ist bezüglich der Rechnungsstellung unabhängig von einem Netzbetreiber und hat eine einfache Möglichkeit, die Abrechnung seiner Dienste in die eigene Hand zu nehmen. Dazu braucht er lediglich eine Einweg-Karte in den Handel zu bringen, über die seine Dienste abgerechnet werden. Die Endgeräte müssen zur Datenverbindung mit dem Datenträger eine geeignete Vorrichtung aufweisen.

[0024] Beispielhaft wird für einen Mehrwertdienst ein Sprachen-Übersetzungsdienst angeführt. Ein solcher Dienst wird nicht permanent in Anspruch genommen, sondern beispielsweise bei einer Konferenz, die eine einmalige Situation darstellt. Der Benutzer würde sich vor Ort eine Prepaid-Karte des Dienstanbieters kaufen und die Dienste nutzen, ohne daß er dafür ein Vertragsverhältnis mit dem Dienstanbieter eingehen muß. Aufgrund der kurzen Dauer der geschäftlichen Beziehung zwischen dem Dienstanbieter und dem Dienstnutzer wäre in diesem Fall eine vertragliche Bindung weder sinnvoll noch wirtschaftlich.

[0025] Es muß nicht zwingend, wie in der in Fig. 2 gezeigten Ausgestaltung des Verfahrens, für jedes Zählerdekrement ein eigener Steuerbefehl gesendet werden. Einfacher und bezüglich der übertragenen Datenmenge effizienter ist es, den Zähler periodisch oder nach einer definierten empfangenen Datenmenge zu erniedrigen und jeweils ein Zählerzertifikat zu erstellen, das dann an das Netzwerk beziehungsweise zur Kontrolleinrichtung gesendet wird. Die Steuerung dieses Verfahrens kann dann im Endgerät durchgeführt werden. Dafür kommt entweder der Controller im Endgerät oder die SIM-Karte in Betracht, indem beispielsweise mit einem Anfangssteuerbefehl ein ausführbares Programm auf die SIM-Karte geladen wird. Bei dieser Implementierung ergibt sich der in der Fig. 3 dargestellte Ablauf.

[0026] Die Fig. 4 und 5 beschreiben eine vorteilhafte Lösung zur Erhöhung der Sicherheit, daß es sich bei dem Dienstnutzer um einen rechtmäßigen Nutzer handelt und nicht ein gefälschter Datenträger verwendet wird. Gemäß dem Beispiel von Fig. 4 wird zusammen mit dem Steuerbefehl von der Kontrolleinheit 8 des Dienstanbieters in kodierter Form die Sendezeit t1 an das Endgerät 3 des Dienstnutzers übermittelt. Die Sendezeit t1 bleibt auch bei Erstellung des Zertifikats erhalten und wird mit dem Antwortsignal an die Kontrolleinheit 8 zurückgesendet. Dort wird die Sende-

zeit t_1 mit der Ankunftszeit t_2 verglichen und der Zeitunterschied Δt ermittelt. Die Zeitdifferenz Δt setzt sich zusammen aus der Zeit der Übertragung von der Kontrolleinheit 8 zu dem Endgerät 3, der Zeit zur Berechnung des Zertifikats und der Übertragungszeit, zurück zur Kontrolleinheit 8. Die Verarbeitungszeit der Zertifikatsberechnung auf dem Datenträger 9 liegt typischerweise bei 30 Millisekunden. Die Übertragungszeiten von der Kontrolleinheit 8 zu dem Endgerät 3 und zurück sind dagegen vernachlässigbar. Der Zeitunterschied Δt gibt daher zuverlässig Auskunft, wie lange die Berechnung des Zertifikats gedauert hat. Die auf dem Datenträger 9 durchgeführten Algorithmen sind in Hardware implementiert. Auf diese Weise ist die Verarbeitungszeit wesentlich schneller als bei softwaregestützter Berechnung, wie sie bei Nachbauten normalerweise eingesetzt wird. Für den Zeitunterschied Δt ergäbe sich somit ein signifikanter Unterschied zwischen einer Originalkarte und einer Nachbildung.

[0027] Überschreitet die Zeitdifferenz Δt einen festgelegten Grenzwert Δt_{max} , bricht die Kontrolleinheit 8 die Verbindung zum Endgerät 3 des Dienstanwenders ab.

[0028] In der Ausführungsvariante von Fig. 5 wird nicht die Sendezeit t_1 mit dem Steuerbefehl übermittelt, sondern eine Kennnummer a . Gleichzeitig wird in der Kontrolleinheit 8 eine Kombination aus der Kennnummer, beispielsweise der Rahmennummer, und der Sendezeit t_1 zwischengespeichert. Die Kennnummer a wird nach der Zertifikatsberechnung mit dem Antwortsignal an die Kontrolleinheit 8 zurückübertragen. Dort wird aus dem Zwischenspeicher 10 die zu der Kennnummer a gehörende Startzeit t_1 ausgelesen und mit der Ankunftszeit t_2 verglichen, woraus sich wieder die Zeitdifferenz Δt ergibt.

[0029] Die Erfindung wurde für den Anwendungsfall eines Mobilfunknetzes und eines Mobilfunkendgerätes beschrieben. Das Verfahren zur Abrechnung von Dienstleistungen zwischen einem Dienstanbieter und einem Dienstanwender in einem Netzwerk ist aber auch auf andere Netzwerke, beispielsweise das Internet, anwendbar. Der Unterschied bestünde hierbei lediglich in dem Übertragungsweg der Informationen. Gegenüber Prepaid-Lösungen in Mobilfunknetzen, wie sie bisher verwendet werden, besteht der große Vorteil, daß nicht eine permanente logische Verbindung notwendig ist, sondern die Informationen zwischen der Kontrolleinrichtung und den Datenträger des Endgerätes paketweise übertragbar sind. Diese paketweise Datenübertragung von Zertifikatsantworten kann als sogenannter Datagram Service, also verbindungslos ausgeführt werden. Die empfangende Kontrolleinrichtung erwartet bei einem zeitgesteuerten Dienst einen kontinuierlichen Fluß der Datenpakete und beendet beim Abbruch dieses Datenflusses nach einer vorgegebenen Wartezeit den Dienst. Die Wartezeit ist abhängig von der zeitlichen Varianz der Datenpakete des Datagram-Services und kann in einer vorteilhaften Ausgestaltung dynamisch an die jeweilige Verbindungsstrecke angepaßt werden.

[0030] Die ausgetauschten Datenmengen sind wesentlich geringer als bei netzzentrierten Guthabenkonto, so daß auch von ausländischen Mobilfunknetzen aus eine Nutzung der Mehrwertdienste sowie deren Abrechnung ohne Probleme möglich ist.

Patentansprüche

1. Netzwerkanordnung mit einem Kommunikationsnetzwerk (1), das eine Kontrolleinrichtung (8) aufweist oder damit verbunden ist, und einem Kommunikationsendgerät (3), **dadurch gekennzeichnet**, daß das Kommunikationsendgerät (3) einen Datenträger (9) mit ei-

nem Zähler (10) aufweist, wobei der Stand des Zählers (10) durch einen Steuerbefehl von der Kontrolleinrichtung (8) änderbar ist.

2. Netzwerkanordnung nach Anspruch 1, dadurch gekennzeichnet, daß der Datenträger (9) eine Datenverarbeitungsschaltung aufweist, die nach der Änderung des Zählerstandes durch Anwendung eines Algorithmus ein Antwortsignal erzeugt, das an die Kontrolleinrichtung (8) übertragen wird.

3. Netzwerkanordnung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß Kommunikationsnetzwerk (1) ein Mobilfunknetz und das Kommunikationsendgerät ein Mobilfunkendgerät ist.

4. Verfahren zur Abrechnung von Dienstleistungen zwischen einem Dienstanbieter (SP) und einem Dienstanwender (SU) in einem Netzwerk unter Verwendung eines Datenträgers (9) durch den Dienstanwender (SU), wobei der Datenträger (9) einen Zähler (10) aufweist und der Dienstanbieter (SP) einen Steuerbefehl an den Datenträger (9) sendet, um dadurch den Stand des Zählers (10) nach festgelegten Kriterien zu ändern.

5. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß der Datenträger (9) nach der Änderung des Zählerstandes ein Antwortsignal an den Dienstanbieter (SP) sendet.

6. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß das Antwortsignal von einem auf dem Datenträger (9) gespeicherten Schlüssel abhängt.

7. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß das Antwortsignal von einem früher gesendeten Antwortsignal abhängt.

8. Verfahren nach einem der Ansprüche 4 bis 6, dadurch gekennzeichnet, daß das Antwortsignal den Zählerstand enthält.

9. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß der Zählerstand nach Zahlung eines Geldbetrages an den Dienstanbieter (SP) auf einen von der Höhe des Geldbetrages abhängenden neuen Anfangszählerstand gesetzt wird.

10. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die Steuersignale zur Änderung des Zählerstandes abhängig von der Zeitdauer einer Verbindung gesendet werden.

11. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die Steuersignale zur Änderung des Zählerstandes abhängig von einer übertragenen Datenmenge gesendet werden.

12. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß jeder Steuerbefehl eine Kennzahl aufweist, die mit dem Antwortsignal zurückgesendet wird, wobei der Dienstanbieter (SP) den Zeitunterschied Δt zwischen Absenden des Steuersignals und Empfang des Antwortsignals auswertet und zur Kontrolle der Verarbeitungszeit des Datenträgers (9) zur Erzeugung des Antwortsignals verwendet.

Hierzu 3 Seite(n) Zeichnungen

- Leerseite -

FIG 1

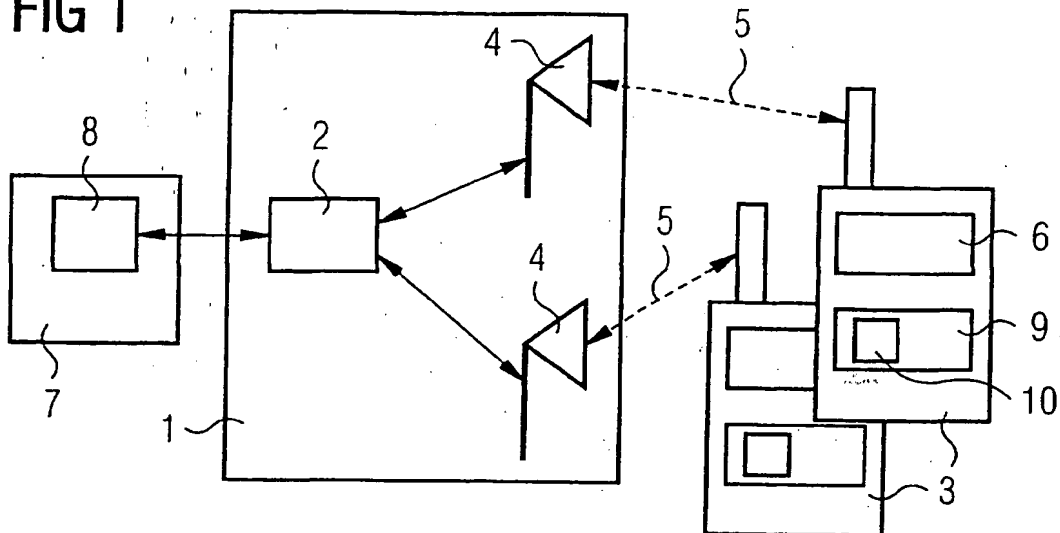


FIG 2

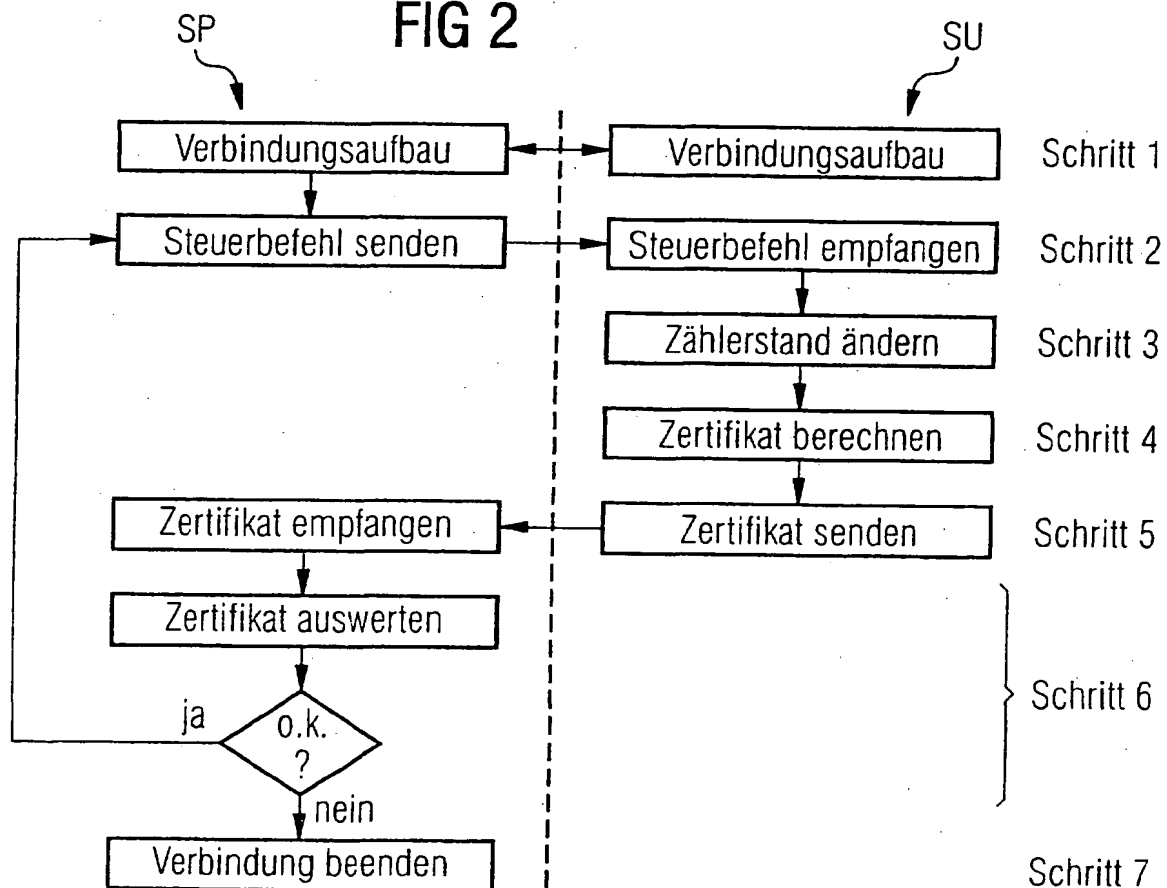


FIG 3

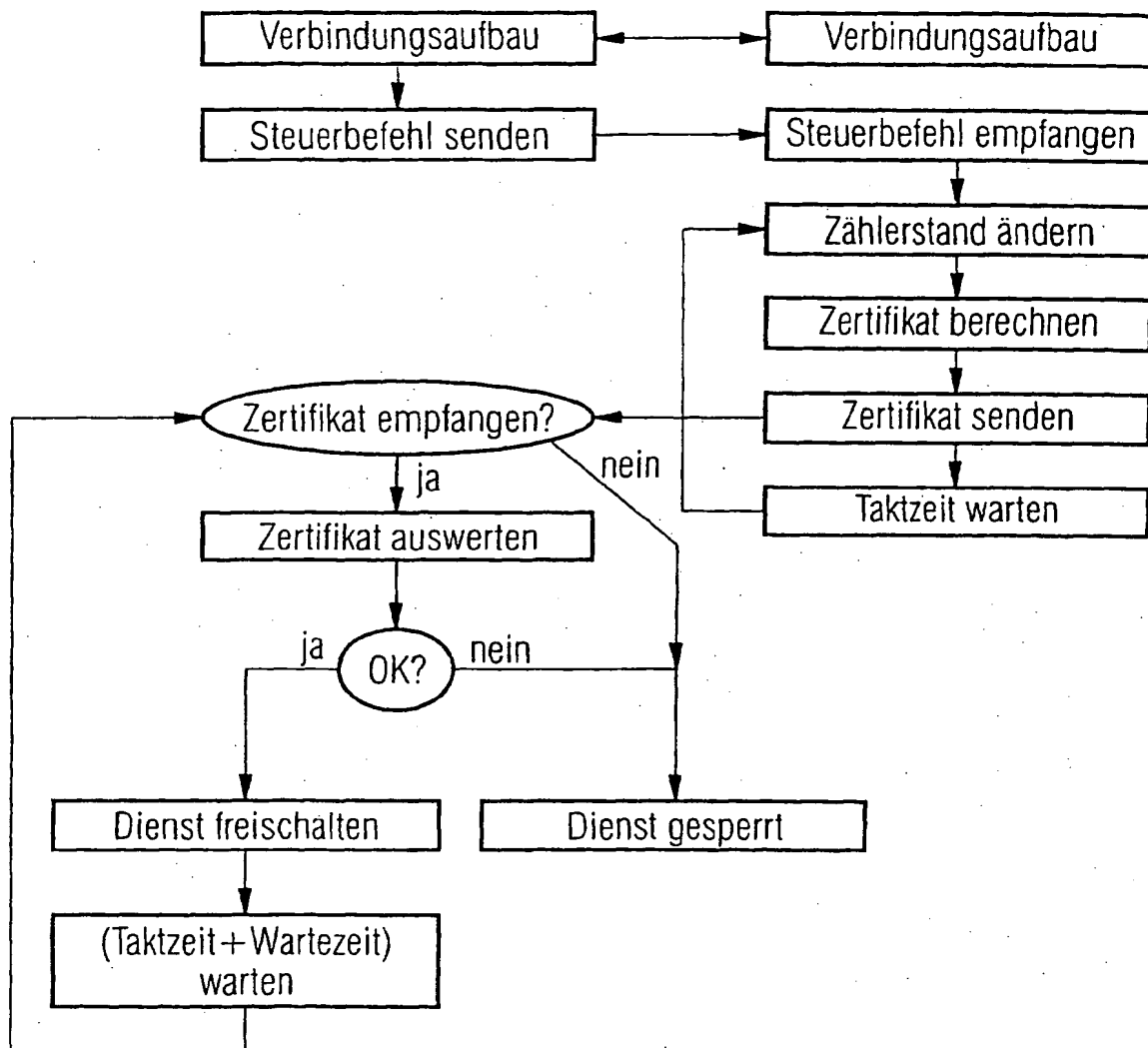


FIG 4

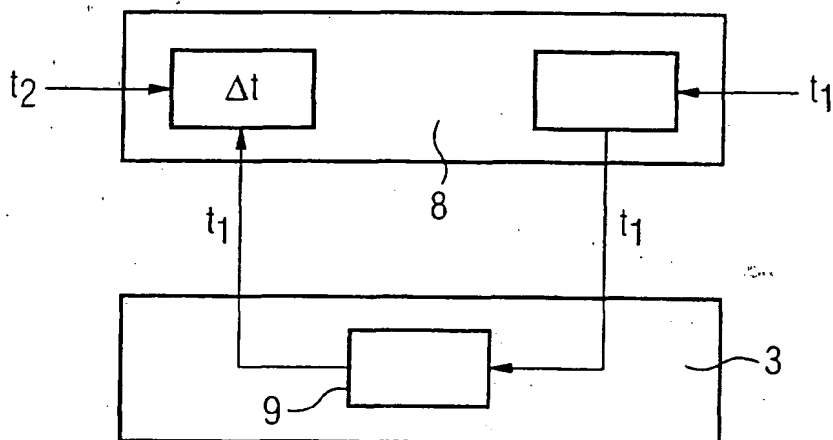


FIG 5

